Método 1: centro de processamento falso
Esse método requer que o autor acesse um cabo conectando a máquina a rede. O hacker desconecta o ATM da rede do banco e o reconecta a um aparelho que se passa por um falso centro de processamento.

A caixa é utilizada para controlar os dispersores de dinheiro além de enviar comandos ao ATM. Simples assim: o autor pode inserir qualquer cartão e senha de modo que a transação parecerá legítima.

Método 2: ataque remoto em diversos ATMs
Envolve um cúmplice do banco. O criminoso adquire uma chave que abre o chassi do caixa. A chave não dá acesso à bandeja de entrega de dinheiro, mas expõe o cabo de rede. O hacker desconecta o ATM da rede do banco e o conecta a um dispositivo especial que envia todos os dados para seu próprio servidor.

Redes que conectam ATMs normalmente não são segmentadas (separadas por segurança) e os próprios caixas podem ser configurados erroneamente. Neste caso, com esse tipo de dispositivo um hacker pode comprometer diversos de uma vez, mesmo se o aparelho malicioso estiver conectado a apenas um deles.

O resto do ataque ocorre como descrito no método 1: um centro de processamento falso é instalado no servidor, e o criminoso ganha controle absoluto dos ATMs. Com um cartão comum, o criminoso pode sacar dinheiro de qualquer caixa. A única coisa que os caixas eletrônicos precisam ter para esse método funcionar é o protocolo utilizado para se conectar ao centro de processamento.

Método 3: o ataque da caixa preta
Como descrito anteriormente, o criminoso obtém a chave para o chassi físico, só que dessa vez coloca a máquina em modo de manutenção. Então, o hacker conecta um dispositivo conhecido como caixa preta em uma das entradas USB expostas – um dispositivo que permite controlar a saída de dinheiro do ATM.

Enquanto o responsável pela fraude altera o ATM, a máquina exibe uma mensagem do tipo “Terminal em Manutenção” ou “Fora de serviço”, mas na verdade ainda pode ser usado para sacar dinheiro. Além disso, a caixa preta pode ser controlada remotamente. O hacker simplesmente aperta um botão para pegar o dinheiro e depois se livra da caixa preta para eliminar evidências.

Método 4: ataque de Malware
Há duas formas de infectar um ATM com malware: basta inserir um pendrive contendo

malware na entrada (o que requer a chave do chassi) ou por infecção remota, ao comprometer primeiro a rede do banco.

Se o ATM alvo não for protegido contra malware ou não emprega métodos de whitelisting, um hacker pode fazer o malware enviar comandos ao caixa e forçá-lo a liberar dinheiro até ficar vazio.

Claro, nem todos os ATMs são suscetíveis a esse tipo de ataque -só é viável se algo estiver errado. Seja a rede do banco que não é segmentada, ou falta autenticação quando o software do ATM troca dados com o hardware, não exista whitelist nos Apps, ou o cabo de rede seja acessível demais.
Infelizmente, esses problemas são bem comuns. Por exemplo, permitiram que os autores infectassem diversos ATMs por meio do Trojan Tyupkin. Especialistas da Kaspersky Lab estão sempre prontos para ajudar bancos a resolver esses problemas: oferecemos consultoria e auditorias de infraestrutura para empresas financeiras, além de conduzir testes de resiliência contra ataques.